Achieving High Confidence of Low Risk

System Assurance Supporting Risk Analysis

Working *Together* to Build Confidence

Richard Mark Soley, Ph.D.
Chairman and CEO

Object Management Group, Inc.

19 September 2012

From *Assurance* to *Trustworthiness*

- **Objective: Effective Measurement of System's Trustworthiness**
  - High confidence of low risk
- **There are plenty of existing Risk Analysis Methodologies**
  - ISO/IEC 13335, ISO/IEC 15408, ISO/IEC 15443, ISO/IEC 27001, CRAMM (UK), EBIOS (France), Mehari (France), Magerit (Spain), HTRA (Canada), NIST SP-800-30 (US), Octave (SEI CMU), RiskAn (Czech Rep), Microsoft Threat analysis Methodology, etc.

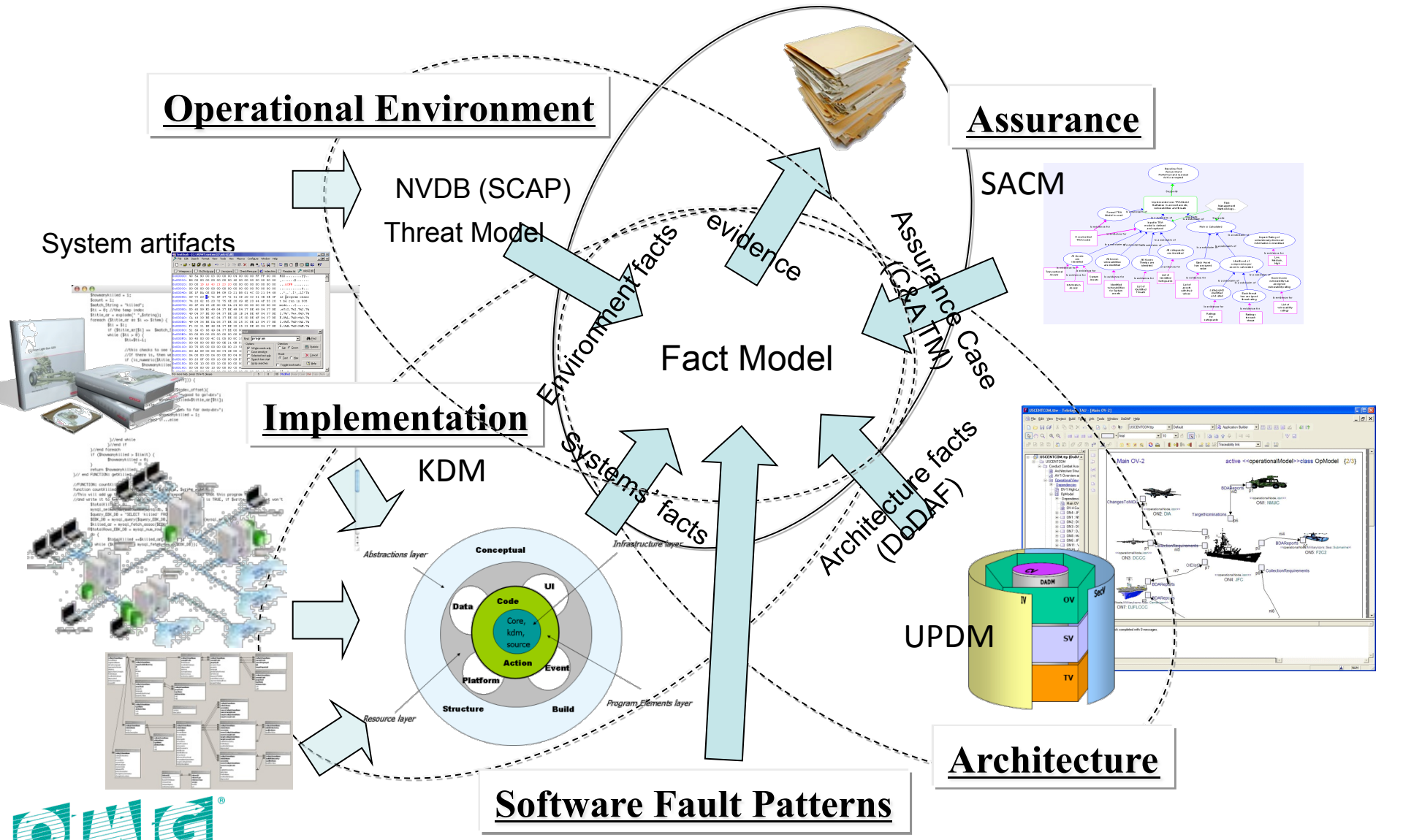
OBJECT MANAGEMENT GROUP

Moving to *Fact-Oriented* Threat/Risk Analysis

1. **Mathematical approach to addressing weakness space – removing** *ambiguity*
2. **Structured, standardized representation of security policies and requirements – providing** *transparency*
3. **Connecting security policies and requirements to the system artifacts that implements them – establishing** *traceability*
4. **Broad tool support – enabling** *automation*
   - No one tool or one vendor can provide solution to address all identified challenges
     - Required set of integrated tools providing end-to-end solution
     - Require arbitration solution to understand what is and is not covered by tools
   - Tools integration possible only through standards
     - Set of standards are needed requiring tight integration between standards
     - Integration of standards require that they are based of the same technology and they follow the rules of technical development
     - The only standard organization producing such interoperability standards is OMG
   - Security Assurance tools' space is fairly young with set of known issues and opportunities
     - Each tool has its strengths and shortcomings
     - Focus: playing on tools strengths and overcoming their shortcoming by integrating them through standards

OBJECT MANAGEMENT GROUP

Common Fact Model: Standards for System Knowledge



OBJECT MANAGEMENT GROUP

OMG Software Assurance Ecosystem

- **A set of *integrated standards***
- **Standard-based tooling environment for analysis and exchange of information related to system assurance and trustworthiness**
  - **dramatically reduces the cost of multi-disciplinary assurance activities**
  - **Based on integrated ISO/OMG Open Standards**
  - **Semantics of Business Vocabulary and Rules (SBVR)**
    - For formally capturing knowledge about weakness space: weaknesses & vulnerabilities
  - **Knowledge Discovery Metamodel (KDM)**
    - Achieving system transparency in unified way
  - **Structure Assurance Case Metamodel (SACM):**
    - Merged the Argumentation Metamodel (ARM) and Software Assurance Evidence Metamodel (SAEM) into one
    - Intended for presenting Assurance Case and providing end-to-end traceability: requirement-to-artifact
  - **Software Metrics Metamodel**
    - Representing libraries of system and assurance metrics
  - **UPDM**
    - Formally representing DoDAF information

OBJECT MANAGEMENT GROUP

A Formal Framework Focusing on Automation

Tools Interoperability and Unified Reporting Environment

Process Docs & Artifacts

Requirements/Design Docs & Artifacts

Reports, Risk Analysis, etc

Process, People & Documentation Evaluation Environment

- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort
- Supported by The Open Group's UDEF*

Process, People, documentation Evidence

Formalized Specifications

Assurance Case Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Supported by the following standards:
- **ISO/IEC 15026**
- **ISO/TC 37 / OMG SBVR**
- **OMG SACM**
- **UPDM**
- Software Fault Patterns

Software System / Architecture Evaluation

- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Supported by OMG KDM (ISO/IEC 19506)

Software system Technical Evidence

Executable Specifications

Software System Artifacts

Hardware Environment

Data Structures

CWE

Security Controls

Protection Profiles